INFORMATION TECHNOLOGY MANUAL

2004

Prepared By:

MONTANA DEPT. OF CORRECTIONS
INFORMATION TECHNOLOGY BUREAU
1539 11TH AVENUE
P.O. BOX 201301
HELENA, MONTANA 59620-1301
(406) 444-3930

MONTANA DEPT. OF CORRECTIONS
POLICY UNIT
1539 11TH AVENUE
P.O. BOX 201301
HELENA, MONTANA 59620-1301
(406) 444-3930

Table of Contents

Table of Contents i
Policy Statement 1
User Responsibility 1
- Requirements 1
- Consent Form 1
- Misuse Of Computer Resources 2
- Reporting and Disciplinary Action 2

Obtaining Computer Assistance 3
Logging On And Off Of The Computer 3
- Logging On 3
- Logging Off 3
- Protecting Unattended Computers 3

User Names and Passwords 4
- User Names 4
- Passwords 4
- Access Rights 4

Email, Internet, and SummitNet Use 5
- General Guidelines 5
- State Provided Electronic Mail (E-Mail) System And Internet Service Acceptable Use 6
- Misuse Of Email / Internet / Computer Services 6
- SummitNet Acceptable Use 7
- Copyright Laws 7
- Internet Filtering 7
- Internet Reporting 8
- Transmission Privacy 8

Remote Access for Employees and Contractors 9
Workstation and Portable Computer Care 9
- Guidelines 9

Workstation, Portable Computer , and PDA (Personal Digital Assistant) Security 9
- Requirements 9
- Guidelines (Not Requirements) 10

Computer Virus Detection and Protection 10
- General Information 10
- Viruses, Hoaxes, Chain Letters And Spam 11

Offender Use of Computers 13
Obtaining a Network, E-mail, or Offender Tracking System Account and Password 13
Computer Training Opportunities 14

Policy Statement

A. Most of the requirements and guidelines in this manual come from the Enterprise Policies listed below. These policies are derived from the governing articles listed at the end of the policy. These governing articles normally are the: MOM (Montana Operations Manual); MCA (Montana Codes Annotated); ARM (Administrative Rules of Montana). **Therefore, violation of these policies may result in disciplinary action including, but not limited to, termination of employment.**

1) ENT-SEC-081, User Responsibility
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec081.asp*
2) ENT-SEC071, Logging On and Off Computer Resources
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec071.asp*
3) ENT-SEC-062, User Names and Passwords
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec062.asp*
4) ENT-NET-042, Electronic Mail
   a) *http://discoveringmontana.com/itsd/policy/policies/entnet042.asp*
5) ENT-SEC-041, Transmission Privacy
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec041.asp*
6) ENT-INT-011, Internet Acceptable Use
   a) *http://discoveringmontana.com/itsd/policy/policies/entint011.asp*
7) ENT-INT-030, Internet Privacy and Security
   a) *http://discoveringmontana.com/itsd/policy/policies/entint030.asp*
8) ENT-NET-031, Summit Net Acceptable Use
   a) *http://discoveringmontana.com/itsd/policy/policies/entnet031.asp*
9) ENT-SEC-090, Internet Reporting
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec090.asp*
10) ENT-SEC-120, Internet Filtering
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec120.asp*
11) S-CC30, Workstation and Portable Computer Care
   a) *http://discoveringmontana.com/itsd/policy/policies/scc30.asp*
12) ENT-SEC-111, Workstation, Portable Computer, PDA (Personal Digital Assistant) Security
   a) *http://discoveringmontana.com/itsd/policy/policies/entsec111.asp*
13) ENT-SEC-101, Computer Virus Detection and Prevention
   a) http://discoveringmontana.com/itsd/policy/policies/entsec101.asp
14) ENT-SEC-130, Remote Access for Employees and Contractors
   a) (*http://discoveringmontana.com/itsd/policy/policies/entsec130.asp*)

B. These Enterprise Policies, as well as additional computer use and administration policies can be found at: *http://discoveringmontana.com/itsd/policy/enterprise.asp*

User Responsibility

- ENT-SEC-081, User Responsibility (*http://discoveringmontana.com/itsd/policy/policies/entsec081.asp*)

Requirements

A. Each user of the State of Montana's computing and information resources should realize the fundamental importance of Departmental information and is responsible for the safe keeping of these resources.
B. User and system administrators must guard against abuses that disrupt or threaten the viability of all systems.
C. Each user is responsible for having knowledge of the State, Agency, and their Facility's policies concerning security and care for their computer.
D. Each user must act responsibly.
   1) Each user is responsible for the integrity of these resources.
   2) Each user must respect the rights of other users by minimizing unnecessary network traffic.
E. State computing facilities and UserIDs are to be used for the job-related activities for which they are assigned.

Consent Form

A. All State employees or contractors with the state who have access to the Internet, e-mail, or other online services, will sign a consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources.

Misuse Of Computer Resources

A. The following items represent, but do not fully define, misuse of computing and information resources:
   1) Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.
   2) Downloading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
   3) Use of computers and UserIDs for which there is no authorization, or use of userIDs for purpose(s) outside of those for which they have been issued.
   4) Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on State-owned equipment.
   5) Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State. (That is, if you abuse the networks to which the State has access or the computers at other sites connected to those networks, the State will treat this matter as an abuse of your computing privileges.)
   6) Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
   7) The use of computing facilities, UserIDs, or computer data for purposes other than those for which they were intended or authorized.
   8) Sending fraudulent e-mail, breaking into another user's e-mail inbox, or unauthorized personnel reading someone else's e-mail without his or her permission.
   9) Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
   10) Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
   11) Taking advantage of another user's naivete or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorization to access.
   12) Physically interfering with other users' access to the State's computing facilities.
   13) Encroaching on or disrupting others' use of the State's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a State computer; damaging or vandalizing State computing facilities, equipment, software, or computer files).
   14) Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
   15) Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
   16) Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

Reporting and Disciplinary Action

A. User will:
   1) Cooperate with system administrator requests for information about computing activities.
   2) Follow agency procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment.
   3) Follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location.
   4) Honor the Acceptable Use Policies of any non-State networks accessed.
   5) Report unacceptable use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.
B. Misuse of the state’s computer resources may result in an agency taking disciplinary action appropriate to the misuse, up to and including termination.

Obtaining Computer Assistance

A. A simple solution to many computer problems is to turn your computer off, wait about one minute and restart. If the error persists after this attempt, contact the Help Desk.
B. All computer assistance calls should go through the Help Desk.
   1) Help Desk phone number: 444-4234 or 1-877-738-4763
   2) Help Desk e-mail: corhelpdesk@state.mt.us
   3) Help Desk DOC Intranet web site: www.my.cor.state.mt.us , then click on "Help Desk"
C. The Help Desk will log the call and assign the call to the appropriate person.

Logging On And Off Of The Computer

- ENT-SEC071, Logging On and Off Computer Resources (*http://discoveringmontana.com/itsd/policy/policies/entsec071.asp*)

Logging On

A. State entities must provide for the security of their data and information resources. This is accomplished by:
   1) Users must properly log on and off the network.
      a) It is an unacceptable practice to bypass normal log on procedures.
   2) Users must not use another employee's User ID and password.
   3) Users may have only one simultaneous connection to the network, unless specifically authorized.
B. All Department computers will have a warning banner displayed at all access points. This banner must warn authorized and unauthorized users of the following:
   1) What is considered proper use of the system.
   2) That the system is being monitored to detect improper use and other illicit activity.
   3) That there is no expectation of privacy while using the system.
C. Common mistakes to avoid when logging on to a computer:
   1) **Passwords are case sensitive.** Ensure that you are not in **Caps Lock** when typing your password.
   2) **You have three attempts to log on to your computer**. If you fail these three attempts your account is disabled until you contact the Help Desk and have them reset your account.
   3) **Not verifying that the username is your username.** If multiple persons use the same computer or if a Help Desk Technician has been on your computer the User Name field in the Network Logon Dialog Box may retain the previous user's information.
   4) **Not reading and comprehending error messages that appear.** Take time to read and understand error messages.
      a) Do not assume it is the same message you have seen before.
      b) The Help Desk will need to know exactly what these messages say if you contact them for assistance.
   5) **Not waiting for the Corrections Explorer program to complete running.**
      a) The Corrections Explorer program inventories the computer and provides automatic updates when required.
      b) Corrections Explorer status is identified by the yellow and red icon resembling the one shown at right.
         (1) The Corrections Explorer icon is located down by the clock in the System Information Area.
      c) If a magnifying glass is seen moving around the image, do not attempt to access any programs. Wait to do anything on the computer until the magnifying glass disappears.

Logging Off

A. Computers should be logged off when not in use.
   1) When users leave work at the end of each day they must logoff the network and power off their workstation(s).
   2) Exceptions include workstations that must be left on to run nighttime jobs.
      a) These computers must be locked or protected by a password protected screen saver to prevent unauthorized access.

Protecting Unattended Computers

A. Computers should not be left unattended while logged onto the state network.
B. Users in secure areas or with access to sensitive information must always log off the network, lock their workstation, or have a password protected screensaver active before leaving their computer unattended.
C. Users leaving their computers unattended for 15 minutes or longer should either:

1) Log off the network.
2) On **Windows 98** computers ensure that the screen is protected with a password protected screen saver.
   a) The screen saver should be set so that after 3 - 5 minutes of inactivity the screen saver will appear and lock the computer from being used without a password.
   b) 3 - 5 minutes is a good value because if you leave your computer unattended due to other business, forgetfulness or an emergency you will be ensured that in just a couple of minutes your computer will be secure.
   c) This might seem a bother, but the consequences of unauthorized personnel accessing the state network is a real threat and needs to be protected against. Also, sensitive data on your computer could be released to other people.
3) On Windows 2000/XP computers lock the workstation.
   a) To lock the workstation press [CTRL] + [ALT] + [Delete] and then select [Lock Workstation]. When the mouse or keyboard is used, a message prompting you to press **[CTRL] + [ALT] + [Delete]** to log on will be displayed.

User Names and Passwords

- ENT-SEC-062, User Names and Passwords (*http://discoveringmontana.com/itsd/policy/policies/entsec062.asp*)

User Names

A. Each user must be identified by a unique ACF2 (Access Control Facility) ID username.
   1) Exceptions must be approved by the agency security officer and documented.
   2) Each username must have a password associated with it.
B. User Names will be suspended if they are not utilized for >90 days or when the individual user no longer requires access. User accounts will be deleted if they have not been utilized for > 180 days. Exceptions to this must be approved by the users supervisor and the agency security officer.
C. Usernames may not be shared.

Passwords

A. Passwords are used to prevent unauthorized personnel from accessing the state computer resources.
B. Passwords will not be written down where they can be found by unauthorized personnel and must not be shared with other individuals.
C. It is recommended that the same password be used for all systems that the user must log on to. The advantage of this is that if only one password is used, it is a lot less likely that it will be written down and found by someone else, compromising the computer network.
D. Passwords must be at least six characters long using a combination of characters containing at least one numeric and one alphabetical character.
   1) Personnel with supervisory, administrative, or super-user authority must have more complex passwords meeting the following requirements:
      a) Minimum of 8 characters
      b) Combination of alpha and numeric characters.
      c) Characters must not be consecutive within the password.
   2) Use of special characters is discouraged since some operating systems/applications can recognize them and others cannot.
E. Never use a password that you use for State of Montana / Department of Corrections network access on the Internet as a logon password to a website.
   1) This potentially compromises our entire network and should be avoided at all costs!
F. Changing Passwords
   1) Do not simply change the number when your password requires changing.
      a) Example: *old password -- user1 new password -- user2* would be unacceptable due to the ease that someone who has compromised your password would have figuring out the new password.
   2) Passwords will be changed at least every 60 days and will not be reused for at least four cycles.
   3) If a user is assigned a new account or has forgotten their password, a new temporary password will be assigned. After initial use, the user must change the password.

Access Rights

A. Access to network resources (programs, data, printers, etc.) is determined by the rights or privileges assigned to each username.

B. If a user changes work positions in an agency, their access rights must be reviewed and changed to match the new job position.
C. Agencies may allow individuals, other than state employees and contractors, access to information for which the agencies are responsible, so long as such access does not violate any license or contractual agreement, state policy or any federal, state, county or local law or ordinance.

Email, Internet, and SummitNet Use

General Guidelines

- ENT-INT-011, Internet Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entint011.asp*)
- ENT-INT-030, Internet Privacy and Security (*http://discoveringmontana.com/itsd/policy/policies/entint030.asp*)
- ENT-NET-031, Summit Net Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entnet031.asp*)
- ENT-NET-042, Electronic Mail (*http://discoveringmontana.com/itsd/policy/policies/entnet042.asp*)
- ENT-SEC-090, Internet Reporting (*http://discoveringmontana.com/itsd/policy/policies/entsec090.asp*)
- ENT-SEC-120, Internet Filtering (*http://discoveringmontana.com/itsd/policy/policies/entsec120.asp*)

A. Usage rules for e-mail and Internet use are similar and will be covered together here.
B. Privacy of e-mail is not guaranteed. Employees should not have expectations of privacy for any messages.
   1) All messages created, sent or retrieved, over the state's systems are the property of the State of Montana.
   2) When drafting and sending e-mail messages, employees should not include anything they are not prepared for the public to read. Statements can potentially become a basis for litigation (e.g. sexual harassment comments) and/or civil or criminal liability. E-mail communication should resemble typical professional and respectful business correspondence.
C. Department Administrators, management and Department of Administration can monitor e-mail for performance, troubleshooting purposes, or if abuses are suspected.
D. Employees should use their best judgment in sending confidential messages over the e-mail system.
   1) The use of encryption should be considered when sending these types of messages.
E. Stationery may be used when it enhances the business content of e-mail. Stationary, moving graphics and /or audio objects should not be used unnecessarily since they consume more resources such as disk space, network bandwidth and tend to detract from the message content.
F. Unsolicited mail, or spam, should be deleted immediately. If delivery of spam persists, the Help Desk should be contacted.
G. Communications sent or received by the e-mail system may be "documents" under Article II, Section 9 of the Montana Constitution or public records under Section 2-6-101, MCA, and should be generated and maintained accordingly.
   1) Employees should delete items from their in-tray and out-tray when they are no longer needed.
   2) If a mail item needs to be retained, it should be moved to an archive folder, a disk, or be printed.
   3) Items placed in an employee's archive are the employee's responsibility.
   4) The need for retention of an item should be reevaluated after it has been stored for 6 months.
   5) Employees can contact the State Records Manager with any questions on retention schedules.
H. Employees should check their mail with a frequency appropriate to their job duties and their departmental policies.
   1) If employees are unable to check their mail for an extended period of time, they should use the Out of Office Assistant auto reply feature or make arrangements to have their mail picked up by someone else (supervisor, secretary, coworker) and reviewed to see if messages need a response.
I. Employees should use care and discretion when sending e-mail to mailing lists and/or large groups.
   1) Sending a large file to multiple recipients could severely impact the network.
   2) When in the address book, if you right click on a group and select "Properties", a dialog box will open to allow you to view the members of that group.
J. The chance of receiving a virus increases with the use of e-mail. Many viruses come embedded in attachments. Suspicious e-mail messages should be forwarded to the State Information Security Manager for investigation before they are opened.
K. Employees should minimize the e-mail features that increase e-mail traffic and should strive to keep message and attachment sizes as small as possible.
   1) Use of graphics in auto-signatures or other parts of messages or attachments should be avoided because they greatly increase the size of a message.
   2) Use of the e-mail text editor for simple messaging tasks is preferred since the same message created in a word processor is much larger.

3) All attachments over one megabyte should be compressed (zipped) prior to sending. If you need to zip a file please contact the help desk to check on the availability of a WinZip license and installation.

State Provided Electronic Mail (E-Mail) System And Internet Service Acceptable Use

- ENT-INT-011, Internet Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entint011.asp*)
- ENT-NET-042, Electronic Mail (*http://discoveringmontana.com/itsd/policy/policies/entnet042.asp*)

A. The following are guidelines for acceptable Internet and e-mail use:
   1) The conduct of state and local government business and delivery of government services.
   2) Transmitting and sharing of information among governmental, research, and educational organizations.
   3) Supporting open research and education in and between national and international research and instructional institutions.
   4) Communicating and exchanging professional information.
   5) Encouraging debate of issues in a specific field of expertise.
   6) Applying for or administering grants or contracts.
   7) Announcing requests for proposals and bids.
   8) Announcing new services for use in research or instruction.
   9) Conducting other appropriate State business.

B. State telephone/telecommunication policies (MOM 1-1103.01 - Personal Telephone Use) apply to use of the state e-mail system. E-mail can be utilized in the same manner as the state telephone/telecommunication system.
   1) Provided for the conduct of state business.
   2) In addition to state business, the state's telecommunication systems may be used by state employees and officials for local and long distance calls to latch-key children, teachers, doctors, day-care centers and baby sitters, to family members to inform them of unexpected schedule changes, and for other essential personal business.
   3) The use of the state's telecommunication systems for essential personal business must be kept to a minimum, and not interfere with the conduct of state business.

C. Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use.

Misuse Of Email / Internet / Computer Services

- ENT-INT-011, Internet Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entint011.asp*)
- ENT-NET-042, Electronic Mail (*http://discoveringmontana.com/itsd/policy/policies/entnet042.asp*)

A. The following items represent, but are not restricted to, the misuse of computer, state e-mail, or internet resources:
   1) Circulating chain letters.
   2) Using the computer, state e-mail system or internet service for:
      a) Non-profit activities.
      b) Non-profit or public, professional or service organization activities that aren't related to an employee's job duties.
      c) Extensive use for private, recreational, or personal activities.
   3) Playing games.
   4) Utilizing Non-State standard software or hardware.
      a) All software and hardware purchases must be approved through the help desk.
   5) Statewide distributions of e-mail.
      a) The system administrator should be contacted for correct procedures for large e-mail distributions.
   6) Using personal e-mail accounts, such as Hotmail, outside of the state provided e-mail system unless an exception has been granted by the State Information Security Officer.
   7) Other misuse activities as referenced in policy ENT-SEC-081, User Responsibilities.

B. The Internet and e-mail has been provided to State employees for the benefit of agencies and their customers. Every State employee has the responsibility to maintain and enhance the State's public image and to use these resources in a productive manner. To ensure these standards are being met, the following guidelines have been established for assisting agencies in developing their agency business use policies for the Internet, intranet and related services.

1) "Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare."
2) Agencies should be in compliance with existing statewide and agency laws, rules and policies. Following are some examples of the existing laws, rules and policies for consideration when creating agency business use policies. Other laws, rules and policies may be applicable.

C. The Communications Decency Act of 1996 makes it a crime to transmit a "communication which is obscene, lewd, lascivious, filthy or indecent with intent to annoy, abuse, threaten or harass another person." This provision applies to all email, even messages sent from one friend or acquaintance to another.

SummitNet Acceptable Use

- ENT-INT-031, SummitNet Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entnet031.asp*)

A. SummitNet (State and Universities of Montana Multi-Protocol Network) is the State's telecommunications nucleus network or backbone connecting agency, University, K-12, library, and local government networks. SummitNet's telecommunications users are elected officials, state and local government employees, educators, students, researchers, authorized contractors, and non-profit organizations. Through SummitNet, these authorized users can access a wide range of national and international information. SummitNet provides connectivity to the Internet, the world's largest network of individuals, governments, organizations, universities, schools, and companies.

B. The following are considered SummitNet Acceptable Use Practices:
1) SummitNet is to be used for: the conduct of state and local government business and delivery of government services; the support of instruction, learning, training, educational administration, research, and grant procurement; the increased participation of citizen oversight of government affairs; and the promotion of economic development.
2) SummitNet users may be subject to restrictive or limited use of the network, including access to the Internet, as determined by a supervising authority or administrator.
3) Any external connections (i.e. Internet service providers, contractors, other non-governmental entities) made to SummitNet and not managed by the Information Services Division must be reported to the State Data Network Manager for compatibility and security reasons.

Copyright Laws

- ENT-INT-011, Internet Acceptable Use (*http://discoveringmontana.com/itsd/policy/policies/entint011.asp*)

A. State employees must honor copyright laws regarding protected commercial software or intellectual property.
1) Duplicating, transmitting, or using software or other electronic property not in compliance with license agreements is considered copyright infringement. State employees are not to make copies of any copyrighted materials without the full legal right to do so. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyrighted material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. In addition, copyrighted agency/State information used on web sites must be clearly labeled as such.

Internet Filtering

- ENT-SEC-120, Internet Filtering (*http://discoveringmontana.com/itsd/policy/policies/entsec120.asp)*

A. The State of Montana ITSD or individual agencies may filter (or block) individual web sites or general classes of sites, such as: radio stations, music distribution sites, proxy servers, groups that include sexually explicit material or hate speech, and personal email sites (such as Hotmail or Yahoo! Mail). The sites or classes of sites filtered are subject to change at any time.
1) Agencies that have particular devices that need access to blocked sites can request that access be provided specifically to them.
2) To request additional filtering or to remove filtering, supervisors should forward their request to the Corrections Help Desk.

B. Computer systems at various facilities within the Department of Corrections may or may not have access to the Internet.
1) Computer systems that are attached to the State Network in secure facilities that are in administrative areas beyond the normal area where offenders are present will normally have full Internet access, Outlook e-mail, and access to other state resources.

2) Computer systems that are inside areas that can be isolated from the offender population by a locked door will normally have access to the State of Montana web pages, including the Department of Corrections Website, Department of Corrections Intranet, and the MINE website and Outlook e-mail.
3) Computer systems that are in close proximity to offenders with no physical locking barrier will not have any Internet access, nor will they have Outlook e-mail capabilities.

Internet Reporting

- ENT-SEC-090, Internet Reporting (*http://discoveringmontana.com/itsd/policy/policies/entsec090.asp*)

A. The reporting of employee Internet access activity may be provided for the following reasons:
   1) Capacity Management
      a) Information Technology Services Division (ITSD) will analyze Internet traffic to ensure there is adequate bandwidth to meet user needs, including adequate response times and within budgeted costs of providing the Internet services.
      b) ITSD staff, during the course of their analysis, will report any access to a site or class of sites that does not appear to be work related and that is of sufficient volume that may be a potential capacity issue to ITSD management.
   2) Department Request
      a) The Department can request (in writing) a report of Internet sites accessed by any employee(s) of the agency.
   4) To request Internet Reporting, supervisors should contact the Corrections Help Desk.
   3) Public Request
      a) Requests for Internet access records of an individual employee by the public will not be honored without the approval of the Director.
   4) Involvement of Law Enforcement
      a) A request from law enforcement for Internet access records cannot be honored without the appropriate court order (search warrant, etc.).
         (1) This does not preclude ITSD or the Department from contacting law enforcement as part of an investigation initiated by either agency.
         (2) Department legal counsel should be consulted whenever a court order is served or an investigation involves contact with law enforcement.

Transmission Privacy

- ENT-SEC-041, Internet Reporting (*http://discoveringmontana.com/itsd/policy/policies/entsec041.asp*)

A. State and federal statutes provide a foundation to guarantee an appropriate level of privacy when electronic communications are used.
   1) Both users of the State of Montana's telecommunications network, and those who provide access, need a common understanding of the levels of confidentiality, security and access provided.
B. The scope of this policy is limited to those activities associated with the "transmission" of information using the State's telecommunications network.
   1) Information transmission is facilitated through local area networks (LANs), wide area networks (WANs) and the voice network.
      a) Such transmissions may include, but not be limited to, electronic documents, electronic files, electronic mail, video, images and voice communications.
C. Transmissions on the State's telecommunications network may only be intercepted (including copying and/or recording) and/or monitored (including viewing and/or listening) when such interception is in the normal course of employment responsibilities, or is regarded as necessary to providing the State's telecommunications services, or is protecting the rights and property of the State of Montana.
   1) Transmissions may be intercepted and/or monitored to conduct mechanical checks, service quality control checks, maintenance of service quality, system security, and software license monitoring.
D. No telephone conversation may be recorded without the knowledge of all parties to the conversation as provided for in 45-8-213, MCA.
   1) State employees who qualify as peace officers may continue, in the course of their duties as law enforcement officers, to record conversations where one party consents (i.e., the officer) to such recordings.
E. No person may intentionally disclose information from intercepted and/or monitored transmissions on the State's telecommunications network except to the person for whom it is intended, to a person reasonably involved in the process of transmitting the information to the person for whom it is intended, or to another person lawfully entitled to it.

F. No person may use information from intercepted and/or monitored transmissions on the State's telecommunications network for any purpose other than supporting and maintaining the State's telecommunications services, or other lawful purposes.
G. If any person is discovered misusing information from intercepted and/or monitored transmissions on the State's telecommunications network, they shall be subject to disciplinary action appropriate to the misuse, up to and including termination as administered under policy 3-0130, Discipline Handling, Montana Operations Manual and possible civil or criminal penalties.

Remote Access for Employees and Contractors

- ENT-SEC-130, Remote Access for Employees and Contractors (*http://discoveringmontana.com/itsd/policy/policies/entsec130.asp*)

A. The appropriate agency administrator must provide requests for remote access for each employee or contractor in writing to ITSD.
B. Remote access users are obligated to abide by all computing policies of the state and the agency.
   1) Access will be granted for legitimate business uses of the State of Montana and not for personal use.
   2) Access to the state's information technology resources by unauthorized remote users will be considered a violation of state policy.

Workstation and Portable Computer Care

- S-CC30, Workstation and Portable Computer Care (*http://discoveringmontana.com/itsd/policy/policies/scc30.asp*)

Guidelines

A. To protect data in the event of power fluctuations or outages, all workstations should be plugged into a surge suppressor or UPS.
B. All computer equipment is vulnerable, especially a keyboard, when liquids are spilled on them.
C. Computer screens and keyboards should be cleaned periodically with a computer non-static cleaner.
   1) Foam cleaner should not be used on computer components.
D. Care should be taken when positioning a computer in the work environment.
   1) The Help Desk should be consulted for proper positioning of hardware.
   2) Computers should be well ventilated.
   3) Electrical cords should be routed so that they are not near heating elements, under file cabinets, or in a manner that may be a hazard for walking.
E. Users must not connect or disconnect computer components while the computer is powered on.
F. Portable computers should be brought to room temperature before using them.
   1) They should not be exposed to extreme cold or heat for any length of time.

Workstation, Portable Computer , and PDA (Personal Digital Assistant) Security

- ENT-SEC-111, Workstation, Portable Computer, and PDA (Personal Digital Assistant) Security (*http://discoveringmontana.com/itsd/policy/policies/entsec111.asp*)

Requirements

A. Users are responsible for maintaining the security of their own computing device and for the following security requirements:
   1) Workstations, portable computers, and PDA's should be kept out of sight and covered when stored in a vehicle.
   2) Any software installed on workstations, portable computers or PDA's that uses script files must not contain a userID or password for the state's computer system.
   3) Workstations with unattended processes running on them must have some type of screen saver with password protection or keyboard locking program enabled on them.
   4) Portable computers MUST be transported as carry on luggage when traveling by plane or bus.
   5) All workstations, portable computers, and PDA's must be updated with the latest security patches, virus scanning software and virus data files. Agencies are responsible for installing patches for high-risk vulnerabilities within 24 hours of notification.
   6) All PDA's used to connect directly to state computers must be state owned. Exceptions to this must be documented and approved by ITSD.

Guidelines (Not Requirements)

A. If highly sensitive or confidential information is stored on a portable computer or PDA, the data should be encrypted.
B. In accordance with ENT-SEC-071, the following information should appear on portable computers when powered on: "This computer is the property of the State of Montana, Department of Corrections and subject to the appropriate use policies located at: http://www.discoveringmontana.com/isd/css/about/statutespolicies.asp. Unauthorized use is a violation of 45-6-311, MCA."
C. Power on or system passwords should be used on workstations that are in highly accessible areas and on portable computers. Power on passwords should be provided to the Network Administrator and kept in a secure place.

Computer Virus Detection and Protection

- ENT-SEC-101, Computer Virus Detection and Protection (*http://discoveringmontana.com/itsd/policy/policies/entsec101.asp*)

General Information

A. Users and network system administrators must guard against viruses that disrupt or threaten the viability of all systems, including those on the State network and those on networks to which State systems are connected. Virus scanning software MUST be installed, updated, and used regularly on servers, workstations, portable computers (and any other computers being used to connect to the state's network remotely), and PDA's (Personal Digital Assistant).
B. Users shall not knowingly introduce a computer virus into a state computer. Using the virus scanning software tools installed on the computer, users MUST scan files and software downloaded from the Internet or from any external source, regardless of its origin. Users must scan ALL diskettes and CD's if they have been used anyplace other than their own workstation.
C. A user that suspects that his/her workstation has been infected by a computer virus must IMMEDIATELY POWER OFF the computer and notify the Help Desk or designated contact person to coordinate virus removal operations. Much of the damage attributed to viruses occurs through improper removal attempts.
D. Most computer viruses are introduced via electronic mail. Virus scanning software has been installed on all enterprise e-mail servers. To avoid virus infiltration, filtering mechanisms may be incorporated without prior notification.
E. Virus scanning software utilizes DAT files to enable them to more easily detect and identify viruses.
    1) It is imperative that these data files are kept up to date.
        a) On State of Montana computers this is done automatically.
        b) The data file dates can be checked by right-clicking on the AntiVirus icon in your system tray (by the clock in the lower right corner of your screen) and selecting the "About" choice on the bottom of the right click menu. Note the date of the file and the version.
            (1) The date should be fairly recent, as these files are continually updated as new virus threats appear.
            (2) The date and version can be checked for most current by going to the web address located in F.2) below.
F. Every State of Montana computer user is entitled (by contract with McAfee) to a free copy of the McAfee Enterprise edition of McAfee Antivirus.
    1) Contact your Help Desk representative for a copy of this. You must provide them with a blank writable CD to transfer the files to you on.
    2) DAT Files can be located at: http://www.discoveringmontana.com/itsd/employee/SEC-virus.asp
G. Guidelines
    1) Suspicious e-mail messages should be forwarded to the Corrections Help Desk for investigation before they are opened.
        a) The Help Desk will forward these to the State Cyber Protection Office if content warrants.
        b) Unsolicited e-mail (Spam) should also be reported to the Help Desk and then deleted.
    2) Users should write protect all diskettes whenever possible. A write-protected diskette cannot be infected unless there is a hardware error that disables the write protection. If the diskette requires write ability, it can be enabled at that time.
    3) Users should not leave diskettes, CD's, or DVD's in the computer when not needed. A PC can become infected from a diskette, CD or DVD left accidentally in a PC if the PC reboots due to an error or the power goes off momentarily. The PC will attempt to boot from the diskette, CD, or DVD in the drive. This can

immediately infect the hard disk if a boot sector virus is present on the diskette, even if the boot process is not successful.

Viruses, Hoaxes, Chain Letters And Spam

A. Viruses
   1) There are several different kinds of computer viruses: boot sector, parasitic, and macro. Boot sector viruses engage their infection just as your computer loads the operating system (as they first come on). Parasitic viruses are also referred to as file infectors, because they infect executable or program files. The combination of a boot sector and parasitic virus are referred to as multipartite viruses. The most recent addition to the virus realm is the macro virus. This virus type is not written in programming code like other viruses. Macro viruses use an instruction set in programs such as Microsoft Word, Outlook and Excel and are often referred to as document viruses. The macro virus becomes active when you open an infected document.

B. Hoax
   1) This type of virus comes in the form of an email message and does not do what it says it does. This is the hoax. The goal of the virus hoax is to get users to pass the message on to as many people as possible, creating traffic on the network and filling up email servers. The following is an example of one of the most popular email hoaxes:

      ```
      VIRUS WARNING !!!!!!

      If you receive an email titled "WIN A HOLIDAY" DO NOT open it.
      ```

   2) Typical signs of a hoax here:
      a) All capital letters with many exclamation points in the title. This is typical of most of the hoaxes (and many scams!) that we see.
      b) A warning to avoid email with a particular title. Almost all of the virus hoaxes contain this type of directive.
   3) The hoax continues:

      ```
      It will erase everything on your hard drive. Forward this letter out
      to as many people as you can.
      ```

   4) Above we see the other classic hoax indication (to forward the hoax to as many people as you can. The hoax now continues:

      ```
      This is a new, very malicious virus and not many people know about it.
      This information was announced yesterday morning from Microsoft;
      ```

   5) A "new" virus would be no big deal. We see over 250 new viruses each month. Microsoft is not in the business of announcing viruses. And the hoax goes on:

      ```
      please share it with everyone that might access the internet. Once
      again, pass this along to EVERYONE in your address book so that this
      may be stopped.
      ```

C. Chain Letter
   1) Chain letters have three recognizable parts: a hook, a threat, and a request. First, there is a hook, to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl Is Dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
   2) When you are hooked, you read on to the threat. Most threats contained in the letter, warn you about the terrible things that will happen if you do not maintain the chain. However, others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
   3) Finally, the request is mentioned. They admonish you to "Distribute this letter to as many people as possible." They never mention clogging the Internet or the local computer network, they only want you to pass it on to others. Here is an example of one of the more popular chain letters:

      ```
      Hi. I am, Michele Cordova, the founder of Bath & Body Works and I want
      your business. We are trying a new advertising campaign through the
      power of YOU, the consumer!
      ```

In order for this to work, you need to send this e-mail to 13 people and I know that is not a lucky number but that is the number we need in order for this to work.

Our computer tracking system will keep count of how many people you send it to so don't feel like you have to send it to thirteen people all at once. You may not send it to the same person more than once unless you internet pals accidentally delete the message, we wouldn't want them to miss out on this great offer. To compensate you for your hard work, we are going to send you a $50 dollar gift certificate redeemable in any store nationwide.

This is not a joke, it will be your loss if you don't send this to 13 PEOPLE.

Thanks again!

>>>>> Michele Cordova

>>>>> Founder of Bath & Body Works

D. Spam
   1) Spam, unsolicited commercial e-mail (UCE), is a growing problem on the Internet. If you have used the Internet for any length of time, you have probably received solicitations via e-mail to purchase products or services. You have not asked for the information, it just suddenly appears in your e-mail in-tray. Spam has caused a new epidemic referred to as Polymailaphobia (the fear of receiving more than 15 e-mail messages per day), and causes some users to waste many hours going through unwanted mail. A popular way to confirm an internet users address is to include a statement to be removed from the mailing list, respond to the message with REMOVE in the subject line. This does not remove you from a list, but confirms it is a legitimate e-mail address that can be sold to companies. E-mail addresses are worth $0.06 each.
   2) The State of Montana uses a tool called Espion Interceptor to capture potential SPAM messages before they reach your inbox.
      a) Espion Interceptor captures potential SPAM and sends a message to your inbox if it receives suspect SPAM every three hours (if potential SPAM is found).
      b) The Espion Interceptor message should be opened and contents analyzed to see if they are SPAM or legitimate mail. Instructions are included as to how to retrieve items from Espion Interceptor.
         (1) This tool is not 100% foolproof and will sometimes let some SPAM through to your inbox and may capture legitimate messages as SPAM.

E. Cookies
   1) Did you know that web sites track such things as when a user last visited, what pages a user accesses, what products a user orders, or a user's password to access a web site? One of the most popular techniques for tracking information such as this is the use of a "cookie".
   2) A cookie is a piece of text placed on a user's hard drive by the browser at the request of a web site. Whenever a user visits a web site, the web server can send a cookie to the user's computer, which is then stored on the hard drive. As the user visits additional sites, more cookies may be added to the hard drive. Each cookie contains information about a user's visit to a specific web site such as an ID number, time of the last visit, pages accessed, and any other information the user gives up willingly. Any time a user registers for anything online, this information is normally stored in a cookie.
   3) A cookie cannot allow a web server to read a user's hard drive, get an E-mail address not given willingly, destroy files on a computer, or create executable programs. Some say the security risk for cookies is very minimal; others say that users could have the same password for their web site access as they do for their login on a network. Since the cookie file is pure text, a password could be received and accessed gained to the network using a valid loginID and password by an outsider. The password used on a network login should be different than a password used on a web site.
   4) There are many convenient and legitimate uses for cookies, but it is hard to tell which ones are good and which ones are not. Some sites, such as Microsoft, do not allow users to access specific areas of their system without allowing a cookie to be put on the user's computer

Offender Use of Computers

- DOC 1.9.3 Offender Access to Computers (I:\DATA\DOC Policies\1-9-3.doc)

A. Under no circumstances will any offender be allowed:
   1) Access to the Internet.
   2) Access to e-mail or any other on-line service such as Microsoft Outlook.
   3) Supervisory or administrative access to file servers.
   4) Access to Wide Area Networks (WANs) (i.e. State of Montana file servers/networks).
   5) Access to non-offender Local Area Networks (LANs) (i.e. MSP/MWP/PHYCF/RYCF/DOC file server/networks).

B. Computers in combined staff/offender use areas must clearly be marked for "Staff Use Only" and "Offender Use"
   1) Offenders must never have access to a staff computer or any computer not labeled "Offender Use" or one that is clearly for staff use.
   2) Offender computer systems must also have a written inventory of computer programs allowed on that computer on a laminated card.
      a) This inventory sheet must be conspicuously attached to the computer.
   3) Offenders may be allowed access to appropriately labeled offender use stand-alone computers and/or freestanding isolated networks at the discretion of the work area supervisor.
   4) Offenders may be allowed access to the offender Virtual Local Area Network (VLAN), with written approval of the Department Computer Security Officer as well as the facility/program Warden/Superintendent/Administrator for work that the offender may perform in Department facilities/programs.
      a) When offenders leave a job assignment, the work supervisor shall notify the Department Computer Security Officer for removal of the offender from VLAN access.

C. Offenders must never have access to any passwords.
   1) Supervisors must maintain all passwords for offender systems.
      a) An offender must never have knowledge of system or program passwords.

D. Supervisors are required to inspect contents of offender computers at least quarterly, by policy.
   1) This inspection must be documented in writing.

E. Staff members supervising offender use of computers should have sufficient knowledge of computer use, particularly in the area of file management and Windows operation, so that they can easily identify offender misuse and properly supervise offender use of computers.

F. Offender Access to Peripherals and Disks
   1) Staff will ensure that offender access to peripherals is limited and closely supervised.
      a) Scanner and Digital Camera use must be reviewed and approved by the supervisor prior to allowing the offender access to the equipment.
   2) Offenders must never have in their possession outside the designated work area (without specific written permission) any computer information-recording device (referred to collectively as "disks"), such as a floppy disk, recordable compact or digital video disk (CD-R, CD-RW, DVD-R, DVD-RW), backup tape, flash memory cards, USB memory sticks, etc.
   3) Strictly Prohibited Offender Disk Usage:
      a) Possession of disks in offender living areas.
      b) Use of disks for personal needs.

Obtaining a Network, E-mail, or Offender Tracking System Account and Password

A. Obtain Training on Information Technology Guidelines
   1) Either:
      a) Attend a Computer Security class.
         (1) Computer Security is included in both the Basic Computer and Windows classes instructed via the Department of Corrections Computer Trainer.
         (2) The Department of Administration (DOA) normally holds a monthly computer security class.
      b) Read this Information Technology Manual.
         (1) The Information Technology Manual is required to be read and signed for, regardless of which method of training is used.
         (2) This manual can be obtained through the Count Office, Computer Trainer, or through the DOC Policy file under: I:\DOC Policies\1-9-1.Att-A.IT Manual.doc.

B. Fill out the required paperwork.
   1) Fill out an *"Information Technology Manual Self Study/User Agreement"* found at the back of the Information Technology Manual.
   2) Fill out (and get approved by your supervisor) a "Network Access Request" form or an "AS/400 - ACIS - PRO-Files Access Request" form.

C. Provide the Information Technology Manual Self Study/User Agreement form and Network Access Request form to the office that processes computer use requests at your facility.
   1) Offices:
      a) MSP – Count Office
      b) TSCTF – Administrative Assistant
      c) BOPP - Administrative Officer
      d) MWP – Administrative Assistant to the Warden
      e) PHYCF – Administrative Officer
      f) RYCF – Facility Administrator
      g) Central Office – Your Bureau Chief
      h) P&P Locations - Central Office P&P Administrative Officer
   2) That office will then process your request to the Department of Corrections Help Desk. The Information Technology Bureau processes standard account requests each Wednesday.

D. You will be notified of your account information and temporary password once it is created.

E. Log on to the resource and change your password in accordance with the password guidelines outlined earlier.

Computer Training Opportunities

A. Computer Training can be obtained through the Department of Corrections Computer Trainer operating out of Montana State Prison.
   1) Phone Extension: (406) 846-1320, extension 2207

B. Basic Computer, Windows Operating System, Microsoft Office (Word, Excel, Outlook, PowerPoint, Access), Internet Research, Computer Security, Offender Tracking Systems, and other classes can be taken in the Computer Lab in the Wallace Building at Montana State Prison or locally via the mobile training lab, when available.
   1) *Most computer classes require a minimum of Windows Operating System familiarity*. This is to ensure that class time is not taken up during advanced classes by teaching basic computer concepts.
   2) The MSP Computer Lab can be accessed through the Command Post after hours through a checkout system or during normal working hours 8 – 4 through the computer trainer.
   3) The mobile computer lab and instructor can be scheduled (usually with a 3 month advance scheduling) to areas remote from Montana State Prison by contacting the computer trainer.

C. Sign up for computer classes by:
   1) Processing a Training Request through your supervisor.
   2) Signing up via the Computer Trainer, Department of Corrections Training, MSP Word Processing, or designated training coordinator at your facility or in your bureau.
   3) When you sign up for a class, it is your responsibility to ensure you make it to the class on time.
      a) If you will not be able to attend, contact the Computer Trainer at extension 2207 as soon as possible to cancel the class in order to allow your slot to be available to others desiring training.

D. Tutoring Sessions can be arranged through the Computer Trainer if necessary, but it is recommended that all computer users take advantage of the learning opportunities provided through the regularly scheduled classes.

INFORMATION TECHNOLOGY MANUAL
In Service Training and Consent Form

Name: _____ Date Reviewed: _____

SSN: _____ Work Location: _____

Shift: _____ Job Title: _____ Supervisor: _____

Work Address: _____

Work Phone number: _____ Date reviewed: _____

In your own words, summarize the information on appropriate use of technologies in the State setting:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

All State employees or contractors with the state who have access to the Internet, e-mail, or other online services, will sign this consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources. Privacy in using the state's computer systems is not guaranteed. Therefore, employees should not have any expectations of privacy when using the Internet, e-mail, or other computer services.

I _____ have read the Information Technology Manual outlining the State of Montana's computer use policies and agree to comply with all terms and conditions. If I have need of clarification on any topic contained within, I understand that I can go to the governing policy listed for clarification. I agree that all network activity conducted while doing State business and being conducted with State resources is the property of the State of Montana.

I understand that the State reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

_____

_____ _____ _____ _____ ☐ ☐

Employee signature Date Supervisor Signature Date Yes No

_____ ☐ ☐ _____ ☐ ☐

Network Administrator Date Yes No Training Bureau Chief Signature Date Yes No

After your supervisor approves this self study by checking the "Yes" box (to indicate your understanding in the summary section), please return this form to the Corrections Help Desk, P.O. Box 201301, Helena, Montana 59620-1301, or to fax number (406) 444-7394.

Once the Network Administrator has reviewed the form it will be sent to the Training Bureau Chief for review and entry into your permanent training record